June 2021

Overview: Space Security: Possible Issues and Potential Solutions

Ziad I. Akir

Space Security:
Possible Issues & Potential Solutions

By Ziad I. Akir
College of Communication
Ohio University

Introduction

Space communication, particularly satellite communication, is becoming an integral component of our overall global telecommunication infrastructure. Satellites are being used for communication, navigation, remote sensing, imaging, and weather forecasting. Satellites are also providing backup communication capabilities when terrestrial communication is interrupted in cases such as earthquakes or other natural (or *unnatural*) disasters. The September 11th events in 2001 demonstrated the value of redundant satellite systems in supporting rescue efforts.[1] Many governments around the world, including the United States, rely on commercial satellite systems for communication, commerce, and defense. Commercial satellite systems include ground-based components such as earth station antennas, data terminals, and mobile terminals; and space-based components include satellites and other systems (e.g. space station and launching vehicles) now essential to global function.

Commercial sectors and governments around the globe have huge investments in space ranging from GEO and LEO satellites to the currently being constructed International Space Station (ISS). These assets are being used to support essential operations such as banking, telecommunication, imaging, manufacturing, and research as well as defense. Moreover, satellites provide services which contemporary human life

---

[1] See Gabriel Martinez, "*Emerging Satellite Systems and Technology*", Presentation, The National Communication Systems, available at:
http://www.ncs.gov/tpos/training/pdf/New%20England/09_SATCOM.ppt

1

and well being have come to depends on such as predicting natural disasters, guiding ships and aircrafts, providing distance education, and telemedicine.

Satellite systems are nevertheless subjected to intentional as well as unintentional threats. These threats may be ground-based, space-based, or interference-based. Threats may appear in the form of natural disasters on earth that can hit terrestrial stations and cause service disruption due to damage or power outage. Environmental threats in space can be due to solar/cosmic radiation or space objects including debris. Finally, solar activity as well as human activities may cause signal interference and jamming of service.

This paper is about security of space systems. My objective is to identify the various vulnerabilities and threats to such systems in space as communication satellites, International Space Station, and space transport (e.g. Space Shuttle), as well as on the ground. Once the issues and threats are identified and explained, the paper will address the various commercial, social, and political consequences of space systems vulnerability. The paper also presents some potential solutions to the various threats to space systems.

Understanding Space Security

Commercial satellite systems are becoming more and more vulnerable to direct physical attack, cyber invasion, and various forms of interference. The mechanical failure of PANAMSAT's Galaxy IV satellite in 1998 disabled around 90% of the paging network in the United States for two to four days.[2] In orbits, satellites face threats from "*space junk*" floating in orbit and from bad weather on earth. A storm may discharge electrical currents that hit power grids and short out transformers and other electrical

---

[2] See "*Wayward Satellite Wreaks Havoc*", Wired News, May 20, 1998. Available at:
http://www.wired.com/news/technology/0,1282,12414,00.html (last visited: *February 26th, 2003*)

systems that operate earth stations and satellite control systems.[3] A listing of natural threats to commercial satellite systems is notes in Table 1.

Natural disasters such as earthquakes, floods, thunderstorms, lightning, dust storms, heavy snow, tropical storms, and tornadoes may damage or destroy ground stations. Ground stations may also be affected by air pollution and bad temperature environments, as well as power failure.

Table 1 *Unintentional Threats to Commercial Satellite Systems* (source: *U.S. General Accounting Office*)

Type of threat	Vulnerable Satellite System Component
Ground-based: Natural occurrences (including earthquakes and floods; adverse temperature environments) Power outage	Ground stations; control centers and data links
Space-based: Space environment (solar, cosmic radiation; temperature variation) Space objects (including debris)	Satellites; control centers and data links
Interference-based: Solar activity; atmospheric and solar disturbances Unintentional human interference (caused by terrestrial and space-based wireless systems)	Satellites; control centers and data links

Satellites in space are vulnerable to space-based environmental changes such as solar and cosmic radiation, solar disturbances, temperature variations, and natural objects (meteoroids and asteroids). The growing number of satellites in space adds to the

---

[3] See "*Protecting Satellites from Stormy Space Weather*", Wireless Newsfactor, September 5, 2002. Available at: http://www.wirelessnewsfactor.com/perl/story/19296.html (last visited: *February 26th, 2003*)

3

problem of space "junk" in the form of spacecraft and debris [4] which increases the probability of collisions in space. [5]

Satellite links are vulnerable to inhospitable conditions such as solar activity and atmospheric disturbances. The increasing number of satellites is putting a high demand on certain frequencies and orbits causing orbital/spectral congestion. Such congestion may lead to unintentional interference to satellite services.

Satellite systems are also vulnerable to intentional human attacks targeting ground stations, satellites in space, or interfere with the tracking and control links. Table 2 shows some of the possible intentional threats that have to be considered.

Table 2 *Intentional Threats to Commercial Satellite Systems* (source: *U.S. General Accounting Office*)

Type of threat	Vulnerable Satellite System Component
Ground-based:	
Physical destruction	Ground stations; communication networks
Sabotage	Links
Space-based (anti-satellite):	
Interceptors (space mines & space-to-space missiles)	Satellites
Directed-energy weapon (e.g. laser, electromagnetic pulses)	Satellites & control center/data links
Interference and content oriented:	
Cyber attacks (malicious software, denial of service, spoofing, data interception)	All system and communication networks
Jamming	All systems

---

[4] See information from the *Satellite Situation Report* from Goddard Space Flight Center, dated September, 1997 and available at: http://liftoff.msfc.nasa.gov/academy/rocket_sci/satellites/ssr.html (last visited: *February 26th, 2003*).

[5] To get a feel of the space junk and man-made debris, see the updated article "*Space Control: Re-entry Assessment and Space Surveillance*", by U.S. Strategic Command. September 30th, 2002. Available at: http://www.stratcom.mil/factsheetshtml/reentryassessment.htm (last visited: *February 26th, 2003*).

4

Ground stations are always under the threat of physical attack, including threats to launch facilities, command and control facilities, and supporting infrastructure. Satellites in space are potential targets for space-based weapons such as space mines (interceptors) and orbiting space-to-space missiles. Moreover, directed energy such as a high-power laser beam can be used to damage or destroy satellite systems and services.[6]

Ground stations, links, and supporting communication networks are all vulnerable to cyber attacks similar to those used in terrestrial computer networks and the Internet. Potential cyber attacks may include viruses, denial of service, unauthorized monitoring and data interception.[7] Attackers can inject fake signals or traffic and have unauthorized access to control services and databases. Earth-to-space links are subject to electronic interference capable of disrupting or denying satellite communication. An attack can *spoof* a satellite receiver by emitting a false signal for deception purposes. False commands given in the telemetry controlling the spacecraft could cause a satellite to move out of assigned orbit and even to destroy itself. It is also possible that viruses injected into terrestrial computer networks associated with space systems could lead to loss of the spacecraft.

Jamming can be used to prevent reception of signals as well as disrupt uplinks, downlinks, and cross-links. Jamming an uplink requires a signal of matching power of the original link being jammed. To do that, large and powerful antennas are needed, which may not be an easy task. Downlink jamming attempts to inject a signal directly into earth terminal receivers. This is generally an easier task than jamming the uplink,

---

[6] The U.S. demonstrated the capability of Mid-infrared Advanced Chemical Laser (MIRACL) to disrupt and destroy satellites. See Department of Defense News Briefing, December 11th, 1997 which is available online at: http://www.fas.org/spp/military/program/asat/t12111997_t1211asd.html

[7] See "Major Satellite hacked in China", *Security* Volume: 2002, Issue: 7, July 1, 2002. pp. 2-3.

and may have far more serious and dangerous consequences. Cross-link jamming is considered the most difficult to achieve. It involves injecting an undesirable signal between two satellites communicating directly with each other in space.

Besides the threat and vulnerability of satellite systems, systems used for launching and servicing satellites are also vulnerable. The *Challenger* disaster[8] during launch in 1986 and the recent breakup of *Columbia* [9] during atmospheric re-entry are both clear evidence of the dangers and risk associated with the various space operations. Failures involving the launching rockets with satellite payloads continue to occur from time to time.[10]

What are the Consequences?

Without doubt, the world is becoming more and more dependent on commercial space systems for economic, social, and military purposes. The question is: What are the consequences of not protecting commercial space systems? To answer this question, the paper addresses first the economic implications. Imagine the annual investments of the commercial space industry. The process of designing, manufacturing, and launching a satellite is a multi-million dollar venture that many countries in the world still cannot afford.[11] Countries that offer launching sites and facilities charge their clients millions of dollars. For example, U.S.-owned satellites represent an investment of more than $100

---

[8] See "*The Challenger Disaster 10 Years Later*" Life Magazine, Available at: http://www.life.com/Life/space/challenger.html (last visited: *February 28th, 2003*).
[9] See the *NASA Web Site* for more details at: http://www.nasa.gov/columbia/ (last visited: *February 27th, 2003*).
[10] See for example the article by Peter Selding "*Harsh Report Issued on Arian 5 Failure*", SpaceNews, January 13, 2003.
[11] See, for example, NASA's report about the International Space Station commercial development, available at: http://commercial.hq.nasa.gov/price/structure.html (last visited February 25, 2003).

6

billion; and the cost of the Space Shuttle *Endeavour* is approximately $2.1 billion.[12] This is a huge investment by the commercial sector as well as governments.

Economic sectors such as telecommunication;, energy and utilities; transportation; and banking and finance; rely on satellite systems. Damage to satellite operations will cause huge and painful monitory losses to the operators of such services. The more dependent countries become on the information and services provided by satellites, the more significant the impact of failure are sure to be. For a country such as the United States, an attack on its commercial satellite systems will create an "Information Pearl Harbor." Such an attack can damage the U.S. economy via its financial markets. Moreover, economic consequences can also be due to hijacking satellite links that provide telephony and television broadcast.

Besides the economic consequences, human lives are at risk due to space systems insecurity. Satellites are used to detect and forecast natural disasters such as storms and tornados. These phenomena can be deadly when societies cannot predict their movement and take precautionary measures ahead of time. Satellites have been doing a good job tracking weather systems and helping forecast hurricanes, tornados, and floods. Remote sensing satellites have been used to study the earth layers and can sometimes help predict earthquakes. Human participants in space projects can also be at risk. Among the best examples are the *Challenger* and *Columbia* Space Shuttle crews who lost their lives due to the failure of their spacecraft. The International Space Station (IIS) and the grounded Russian Space Station (MIR) before it housed humans for extended periods of time.

---

[12] See, "The Space Shuttle General Information", available at:
http://seds.lpl.arizona.edu/ssa/docs/Space.Shuttle/general.shtml (last visited June 5th, 2003).

7

Securing and protecting these stations is high on the agenda of those involved in space development.

Lack of space security can have social consequences when signals are spoofed or jammed causing disruption to social services. Sometimes, as with telemedicine, human lives can be jeopardized when remote medical diagnosis and surgery cannot be preformed due to lack of satellite links. Tampering with satellite television signals can have social consequences as well. Intentional or unintentional signal spoofing can send the wrong program/content to the wrong intended destination.[13] The increasing access to the Internet via satellite systems put some societies at a higher risk. Computer viruses can be transmitted via satellite systems and cause huge computer system damage and data exposure.[14]

Commercial space systems are vital in support of military and other governmental operations and activities. Military forces can often operate in environments with little or no existing communication infrastructure. Collecting information in the form of mapping and real-time movements of enemy forces is of crucial importance. Commercial satellite imagery systems are used by governments to achieve their national security interests.[15] During the U.S. showdown with Iraq earlier this year, the U.S. government used satellites to track the movement of the Iraqi military as well as keeping track on the where-abouts

---

[13] See "*Arabsat porn in Arabic countries no more*" ArabicNews.com. Available at: http://www.arabicnews.com/ansub/Daily/Day/970723/1997072308.html (last viewed February 27, 2003)
[14] See "Satellite Anti-Virus Protection, *Computer Fraud & Security*, Volume: 2000, Issue: 11, November 1, 2000. pp. 4.
[15] See Jason Bates "*U.S. Commits to Purchase Commercial Satellite Imagery*", SpaceNews, January 20, 2003.

8

of the Iraqi weapons.[16] Failure in commercial satellite operation may have devastating consequences on the outcome of a military or political conflict.

Potential Solutions & Recommendations

In light of the importance of space systems to national and international economies, the growing reliance on them, and the threats that face them, governments around the globe are recommended to explore the various security techniques available to protect satellite systems from unauthorized use, disruption, or damage. The president of India issued a call for an international space force to protect satellites from any war that may spill into space.[17]   The U.S. Air Force Space Command's new master plan envisions new space systems to protect American assets in space.[18]

The space arena needs an organization to properly assure safety, enforce laws, protect the environment, and conduct security operations. This organization should be multi-national since space law is founded primarily on international treaties and agreements. Such an organization should have the means to operate as a global space police force to ensure space security.

Satellite system engineers will need to think of new protective materials that can better shield satellites from atmospheric and environmental attacks. Some military satellites today are "hardened" to protect them against electromagnetic pulse radiation and against collision with micro-debris. Commercial satellites need similar protection to protect them and extend their life. The growth in space junk and the growth in

---

[16] See "*Satellites Spying On Iraq Available On 'Net*" NewsChannel2000, available at: http://www.wesh.com/spacenews/1793089/detail.html (last visited February 27, 2003)

[17] See "*India's President Calls For Space Force to Protect Satellites*" SpaceNews, January 13, 2003.

[18] See Jermy Singer "*U.S. Air Force Plan Re-emphasizes Space-Based Weapons*", SpaceNews, February 3, 2003.

9

worldwide commercial and military satellite systems activities require some sort of space traffic system. Such a system will be needed to control the traffic in and around high-value spacecrafts such as the Space Station as well as control traffic in populated orbits. For out-of-service satellites, the U.S. Federal Communication Commission (FCC) is working on rules for debris migration by U.S. commercial users.[19] These rules will require that satellite companies boost satellites that are beyond their service lives into high "parking" orbits where they will sit for thousands of years. Alternatively, companies can de-orbit their satellites back to Earth where they will burn up in the Earth's atmosphere.

Commercial satellite companies should also take into consideration the location and design of their satellite Earth stations in order to minimize possible damage due to natural disasters such as earthquakes, storms, and floods. Moreover, physical security of these stations is needed to protect against terrorist activities and other intentional attacks.

Better encryption techniques and algorithms are needed to prevent link hijacking and signal spoofing. Techniques used by television operators to scramble un-paid-for services can be used to jam dangerous frequencies. With the increase in popularity of digital signal processing, such algorithms are becoming more powerful in securing uplinks and downlinks alike.

Finally, protecting the space environment will benefit all mankind. Despite the fact that certain nations are only looking to dominate space in order to serve their national interest and political gain, it is the duty of all nations to join together in a peaceful effort

---

[19] See Clay Moltz, "*Future Space Security*", Nuclear Threat Initiative. June 2002, available at: http://www.nti.org/e_research/e3_13b.html (last viewed on February 27, 2003).

10

and look at space as our future arena for scientific and technological exploration to

benefit all humanity.

Further References

U.S. Air Force (1995) "*New World Vistas Air and Space Power for the 21st Century*", Available Online at: http://www.fas.org/spp/military/docops/usaf/vistas/vistas.htm

Bruce Elbert (1999), *Introduction to Satellite Communication*, 2nd Edition, Boston: Artech House.

United State General Accounting Office, (2002) "*Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed*".

Charles H. Cynamon, (1999) "*Protecting Commercial Space Systems: A Critical National Security Issue*", Research Report.

Peter Grier (September 1996), "The Arena of Space", *Air Force Magazine*.

Suzuki, Y., Wakana, H., Takashi, I. (2002), "Future Vision of Satellite Communications for Expanding Human Activities", *Acta Astronautica*, Vol. 51 (1-9), pp. 621-626.

U.N. General Assembly (1999) "*National research on space debris, safety of nuclear-powered satellites, and problems of collisions of sources with space debris*", Committee on the Peaceful Uses of Outer Space.

11